

EE 599 -- Quantum Information and Quantum Computation

Topics for Individual Projects

Communication Protocols

Quantum channel capacity. *This is several problems: how much classical information can be sent using quantum channels? How much if we also allow shared entanglement? How much quantum information can be sent? How much with shared entanglement? With a shared classical channel?*

Quantum bit commitment. *Can Alice provide Bob with a bit value in such a way that Bob cannot read the bit until Alice gives him a key, but Alice cannot change her mind about the bit value? This is impossible classically and quantum mechanically.*

Security proofs for quantum cryptography.

Quantum communication complexity. *Alice has a number x and Bob a number y ; they wish to compute a number $f(x,y)$ with the minimum amount of communication.*

Quantum secret sharing. *A quantum state is divided among several people in such a way that any n of them can reconstruct the state, but fewer than n of them cannot.*

Decoherence, Noise, and Error Correction

Stabilizer codes for quantum error correction. *These are the quantum equivalent of classical check-sum codes, used to protect computers from decoherence. They have an interesting group structure.*

Fault-tolerant quantum computation. *For sufficiently low decoherence/error rates per step, a quantum computation of unlimited length can be done with only polynomial overhead for error correction.*

Decoherence-free subspaces. *For decoherence with certain symmetries, there are subspaces of Hilbert space which are totally unaffected. By imbedding a quantum computation in this subspace, it will be immune to noise.*

Algorithms and Information Processing

Universal sets of quantum gates.

Computational complexity classes for quantum computers.

The Hidden Subgroup Problem. *Given a group G and a function f which is constant on a subgroup K , find a generating set for K .*

Optimal quantum cloning. *Quantum states cannot be cloned exactly. How well can they be cloned approximately?*

Quantum Random Walks. *These are unitary analogues of classical random walks; instead of moving right or left with some probability, the move with some amplitude, and hence can exhibit interference.*

Quantum games. *Quantum analogues of two-player games in Game Theory, in which superpositions of strategies are allowed.*

Simulating quantum systems with quantum computers.

Other Models of Quantum Computation

Quantum Turing Machines.

Cluster State quantum computing. *By preparing a special, highly-entangled initial state of many q-bits arranged on a lattice, quantum computation can be done using only single-bit measurements.*

Adiabatic quantum computing. *Some NP-hard problems are equivalent to finding the minimum eigenvalue of a Hamiltonian. One starts in the known ground state of one Hamiltonian and slowly alters it to be the desired Hamiltonian; if slow enough, the system will remain in the (instantaneous) ground state at all times.*

Quantum computation using only measurements. *If one can prepare ancillas in the states $|0\rangle$ and $|1\rangle$ and do any two-bit measurement, it is possible to do general quantum computations without any unitaries.*

Information Measures for Quantum Mechanics

Quantifying entanglement. *Given an entangled state, can we quantify how entangled it is? Under what circumstances can one entangled state be transformed to another using only local operations and classical communication (LOCC)?*

Practical implementations of QIP

Ion traps

NMR

Solid state (quantum dots)

Solid state (superconducting)

Linear optics

Building gates from physical interactions. *Given a physical system whose*

subsystems interact in a particular way, how can we use this interaction to produce controllable gates?